AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR AN ARREST WARRANT

I, Michael Agostinho, a Special Agent with Homeland Security Investigations, being duly sworn, depose and state as follows:

1. I have been employed as a Special Agent ("SA") of the U.S. Department of Homeland Security, Homeland Security Investigations ("HSI"), since 2008, and am currently assigned to the Office of the Resident Agent in Charge, Providence, RI. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media.

2. As a federal agent, I am authorized to investigate violations of laws of the United States, including 18 U.S.C. §§ 2251, 2252, and 2252A, and to request and execute search or arrest warrants issued under the authority of the United States.

3. I make this affidavit in support of an application for a criminal complaint against John Daniel Macintyre, year of birth 1989, of 38 Landis Drive, East Greenwich, RI 02818, charging Macintyre with violations of 18 USC § 2252A(a)(5)(B).

a. Title 18 U.S.C. §§ 2252A(a)(5)(B) prohibits a person from knowingly possessing or knowingly accessing with intent to view any material that contains any visual depiction involving the use of a minor engaging in sexually explicit conduct, or an image of child pornography as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using

any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

4. The information contained in this affidavit is based on an investigation conducted by this affiant and information obtained by this affiant from other law enforcement officers involved in this investigation.

5. This affidavit is being submitted for the limited purpose of establishing probable cause to secure a criminal complaint and arrest warrant. In submitting this affidavit, I have attempted to summarize the most relevant facts that establish the requisite probable cause. Therefore, I have not included each and every fact of this investigation. Additionally, where conversations or statements are related herein, they are set forth in substance and in pertinent part.

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

6. Your affiant learned that a user of the Internet account at 38 Landis Dr, East Greenwich, RI 02818 has been linked to an online community of individuals who regularly send and receive child pornography via a hidden service website that operated on the Tor anonymity network. The website is described below and referred to herein as the "TARGET WEBSITE."[1]

The Tor Network

[1] The name of the TARGET WEBSITE is known to law enforcement. Investigation into the users of the website remains ongoing and disclosure of the name of the website would potentially alert active website users to the investigation, potentially provoking users to notify other users of law enforcement action, flee, and/or destroy evidence.

7. The Internet is a global network of computers and other devices. Devices directly connected to the Internet are uniquely identified by IP addresses, which are used to route information between Internet-connected devices. Generally, when one device requests information from a second device, the requesting device specifies its own IP address so that the responding device knows where to send its response. On the Internet, data transferred between devices is split into discrete packets, each of which has two parts: a header with non-content routing and control information, such as the packet's source and destination IP addresses; and a payload, which generally contains user data or the content of a communication.

8. The website further described below operated on the Tor network, which is a computer network available to Internet users that is designed specifically to facilitate anonymous communication over the Internet. The Tor network attempts to do this by routing Tor user communications through a globally distributed network of relay computers, along a randomly assigned path known as a "circuit." Because of the way the Tor network routes communications through the relay computers, traditional IP address-based identification techniques are not effective.

9. To access the Tor network, a user must install Tor software. That is most easily done by downloading the free "Tor browser" from the Tor Project, the private entity that maintains the Tor network, via their website at www.torproject.org.[2] The

[2] Tor users may also choose to manually configure a web browser or other application to route communications through the Tor network.

Tor browser is a web browser that is configured to route a user's Internet traffic through the Tor network.

10. As with other Internet communications, a Tor user's communications are split into packets containing header information and a payload and are routed using IP addresses. In order for a Tor user's communications to be routed through the Tor network, a Tor user necessarily (and voluntarily) shares the user's IP address with Tor network relay computers, which are called "nodes." This routing information is stored in the header portion of the packet. As the packets travel through the Tor network, each node is able to see the address information of the previous node the communication came from and the next node the information should be sent to. Those Tor nodes are operated by volunteers – individuals or entities who have donated computers or computing power to the Tor network in order for it to operate.

11. Tor may be used to access open-Internet websites like www.justice.gov. Because a Tor user's communications are routed through multiple nodes before reaching their destination, when a Tor user accesses such an Internet website, only the IP address of the last relay computer (the "exit node"), as opposed to the Tor user's actual IP address, appears on that website's IP address log. In addition, the content of a Tor user's communications is encrypted while the communication passes through the Tor network. That can prevent the operator of a Tor node from observing the content (but not the routing information) of other Tor users' communications.

12. The Tor Project maintains a publicly available frequently asked questions (FAQ) page, accessible from its website, with information about the Tor network.

Within those FAQ, the Tor Project advises Tor users that the first Tor relay to which a user connects can see the Tor user's actual IP address. In addition, the FAQ also cautions Tor users that the use of the Tor network does not render a user's communications totally anonymous. For example, in the Tor Project's FAQ, the question "So I'm totally anonymous if I use Tor?" is asked, to which the response is, in bold text, "No."

13. The Tor Network also makes it possible for users to operate or access websites that are accessible only to users operating within the Tor network. Such websites are called "hidden services" or "onion services." They operate in a manner that attempts to conceal the true IP address of the computer hosting the website. Like other websites, hidden services are hosted on computer servers that communicate through IP addresses. However, hidden services have unique technical features that attempt to conceal the computer server's location.

14. Unlike standard Internet websites, a Tor-based web address is comprised of a series of either 16 or 56 algorithm-generated characters, for example "asdlk8fs9dflku7f," followed by the suffix ".onion." Ordinarily, investigators can determine the IP address of the computer server hosting a website (such as www.justice.gov) by simply looking it up on a publicly available Domain Name System ("DNS") listing. Unlike ordinary Internet websites, however, there is no publicly available DNS listing through which one can query the IP address of a computer server that hosts a Tor hidden service. So, while law enforcement agents can often view and access hidden services that are facilitating illegal activity, they cannot determine the IP

address of a Tor hidden service computer server via public lookups. Additionally, as with all Tor communications, communications between users' computers and a Tor hidden service webserver are routed through a series of intermediary computers. Accordingly, neither law enforcement nor hidden-service users can use public lookups or ordinary investigative means to determine the true IP address – and therefore the location – of a computer server that hosts a hidden service.

Description of TARGET WEBSITE

15. The TARGET WEBSITE is a known darkweb site that contained child sexual abuse material and facilitated the sharing of that material. This website appeared to facilitate the sharing of child abuse material (images, links, and videos), with an explicit focus on indecent material depicting boys.

16. Users were able to view some material on the website without creating an account, but an account was required to post material to the site and to access all the site's content. Postings to the TARGET WEBSITE that were publicly available to any registered user of the TARGET WEBSITE were captured and archived for law enforcement review. Review of such postings disclosed the following posts, among others, by TARGET WEBSITE users:

a. File name: 865219MATRIX061618SEGRaamat10yoanal40yo06.PNG

Description: The file is a .png file that depicts a prepubescent male penetrating an adult male's anus.

b. File name: alex-anal02.jpg

Description: The file is a .jpg file that depicts a prepubescent male's exposed penis with an adult male's penis lying next to it.

Evidence Related to Identification of Target that Accessed TARGET WEBSITE

17. I am aware that U.S. as well as foreign law enforcement agencies investigate anonymous offenders engaging in online child sexual exploitation via Tor hidden service websites such as the website(s) described herein. Those websites are globally accessible. The websites and their users may therefore be located anywhere in the world. Due to the anonymity provided by the Tor network, it can be difficult or impossible to determine, at the beginning of an investigation, where in the world a particular website or user is located. Accordingly, when a law enforcement agency obtains evidence that such a website or website user may be located in another country, it is common practice for that law enforcement agency to share information with a law enforcement agency in the country where the website is located or the offender appears to reside, in accordance with each country's laws.

18. In August 2019, a foreign law enforcement agency (referenced herein as "FLA") known to the FBI and with a history of providing reliable, accurate information in the past, notified the FBI that FLA determined that on April 23, 2019, IP address 68.0.205.247 "was used to access online child sexual abuse and exploitation material" via the website that the FLA named and described as the TARGET WEBSITE (described in paragraph 15).

19. FLA described the darkweb site as having "an explicit focus on the facilitation of sharing child abuse material (images, links and videos), emphasis on

indecent material of boys," stated that "[u]sers were able to view some material without creating an account. However, an account was required to post and access all content," and provided further documentation naming the darkweb website as the TARGET WEBSITE, which the FLA referred to by its actual name.

20. FLA is a national law enforcement agency of a country with an established rule of law. There is a long history of U.S. law enforcement sharing criminal investigative information with FLA and FLA sharing criminal investigative information with U.S. law enforcement, across disciplines and including the investigation of crimes against children. FLA advised U.S. law enforcement that it obtained that information through independent investigation that was lawfully authorized in FLA's country pursuant to its national laws. FLA further advised U.S. law enforcement that FLA had not interfered with, accessed, searched, or seized any data from any computer in the United States in order to obtain that IP address information. U.S. law enforcement personnel did not participate in the investigative work through which FLA identified the IP address information provided by FLA.

21. I am aware through my training and experience and consultation with other U.S. law enforcement agents that tips provided by FLA regarding IP addresses that FLA advised were associated with access to Tor network child exploitation-related web and chat sites have: (1) led to the identification and arrest of a U.S.-based child pornography producer and hands-on offender, and the identification and rescue of multiple U.S. children subject to that offender's ongoing abuse; (2) led to the seizure of evidence of child pornography trafficking and possession; and (3) been determined

through further investigation to be related to targets that U.S. law enforcement investigation had independently determined were associated with child pornography trafficking and possession.

22. As described herein, the TARGET WEBSITE could not generally be accessed through the traditional internet. Only a user who had installed the appropriate Tor software on the user's computer could access the "TARGET WEBSITE." Even after connecting to the Tor network, however, a user would have to find the 16-or-56-character web address of the TARGET WEBSITE in order to access it. Hidden service websites on the Tor Network are not "indexed" by search engines—such as Google—to anywhere near the same degree as websites that operate on the open Internet. Accordingly, it is much more difficult to perform a Google-type search of hidden service websites than it is to search open Internet websites for particular content of interest. Users interested in accessing child exploitation material (or in advertising child exploitation and pornography websites they operate) therefore keep, maintain, and use directory sites that advertise the web addresses of hidden services that contain child exploitation related content. Those directory sites also operate via the Tor network. Users utilize those directory sites to identify new web forums, chat sites, image galleries and file hosts pertaining to the sexual exploitation of children. Such directory sites often identify whether particular sites are then operating, whether child pornography imagery may be found there, and even what types of child pornography are accessible (i.e., boys, girls, or "hurtcore"). They also contain clickable hyperlinks to access those sites. As with other hidden service websites, a user must find the 16-or-56-

character web address for a directory website in order to access it. While it operated, the web address for the website described herein was listed on one or more of such directory sites advertising hidden services dedicated to the sexual exploitation of children.

23. I am also aware through consultation with FBI agents that the review of detailed user data related to one Tor network-based child pornography website found that it was exceedingly rare for a registered website user to access that website and never return. FBI review of user data from that website found that less than two hundredths of one percent of user accounts registered an account on the website, accessed a message thread on the website, and then never returned to the website and logged in to the same account.

24. Accordingly, based on my training and experience and the information articulated herein, because accessing the TARGET WEBSITE required numerous affirmative steps by the user – to include downloading Tor software, accessing the Tor network, finding the web address for TARGET WEBSITE, and then connecting to TARGET WEBSITE via Tor – it is extremely unlikely that any user could simply stumble upon TARGET WEBSITE without understanding its purpose and content.

25. Accordingly, for all of the reasons described herein, I had probable cause to believe that, any user who accessed the TARGET WEBSITE had, at a minimum, knowingly accessed the TARGET WEBSITE with intent to view child pornography or attempted to do so.

Identification of SUBJECT PREMISES

26. According the publicly available information, IP address 68.0.205.247 – the one used to access TARGET WEBSITE, as described above – is owned/operated by Cox. On or about November 22, 2019 a summons was served on Cox for the subscriber assigned IP address: 68.0.205.247 on April 23, 2019 at 01:50:24 UTC. Cox provided their response with the following subscriber details:

Subscriber Name: Daniel MacIntyre
Service Address: 38 Landis Dr East Greenwich, RI 02818
Home Phone: 401-884-XXXX
Method of Payment: eCheck 23045604 A
Account Status: Active (A)

27. Further investigation of databases, DMV records, and utility records revealed that 38 Landis Dr East Greenwich, RI 02818 was owned and occupied by Daniel MacIntyre, year of birth 1962, and his wife Maria MacIntyre, year of birth 1962. Other possible occupants of the property were John MacIntyre, year of birth of 1989, and Katelyn MacIntyre, year of birth of 1995.

SEARCH WARRANT ACQUISITION AND EXECUTION

28. On March 5, 2021, United States Magistrate Judge Lincoln D. Almond signed a search warrant authorizing the search of 38 Landis Dr, East Greenwich, RI 02818 for evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of 18 U.S.C. § § 2252(a)(4)(B) and 2252A(a)(5)(B)."

29. On March 17, 2021, your affiant and other law enforcement agents executed the warrant at 38 Landis Dr, East Greenwich, RI 02818. Present at the residence at the time of the warrant execution were Daniel MacIntyre, John MacIntyre, and Katelyn MacIntyre. Maria MacIntyre left the residence for work immediately before the execution of the warrant but was stopped by law enforcement and returned to the residence following the execution of the warrant.

30. During the search of the residence, a number of computers and hard drives were located in what was later determined to be the bedroom of John McIntyre. Seized from his bedroom: 1 Acer laptop computer, 11 hard drives – 2 external drives and 9 internal drives, 2 of which had been removed from a desktop computer, and 1 Samsung cellular phone.

31. On premises, Rhode Island State Police Computer Forensics Analyst Gerald Gent performed a live preview of the Acer N17C1 laptop computer, serial number NHQ28AA00174405C5C340. As a result of the preview, he observed several videos of child pornography [3] stored in \Users\jmedi\Downloads\New Folder\ and

[3] "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

evidence of the Tor browser being installed on the computer. He noted one video, in particular, named no1_AmlaGoodBoyBro.mp4, depicting juvenile males graphically exposing and manipulating their genitals and engaged in sexual acts with other juvenile males.

32. Agents spoke with John McIntyre on scene in his parents' bedroom while the other occupants of the home remained in the kitchen. Before speaking with John McIntyre, agents orally advised him of his *Miranda* rights, which he acknowledged understanding. Additionally, he was given a pre-printed form containing his Miranda rights, which he reviewed and signed, acknowledging that he understood his rights. He thereafter voluntarily waived his rights and agreed to speak with agents.

33. During the ensuing conversation, John McIntyre, in pertinent part, admitted to utilizing the TOR network to access the darkweb to view child pornography over the past 6 years. He indicated that he viewed child pornography between 2 to 3 times a week, for sexual gratification. He stated that there were approximately 5 videos on his laptop that he had viewed last night. McIntyre stated that he usually views videos and then deletes them after he views them, so there could be hundreds of deleted child-pornographic videos on his laptop. McIntyre stated that he has been viewing child pornography over the past 15 years and has used peer to peer (P2P) applications to do so, such as Limewire. Further, he admitted that he has a sexual preference for prepubescent children, and admitted to having a problem with child pornography, and had tried to stop viewing it in the past.

CONCLUSION

34. Based upon my training, experience, and knowledge of the investigation, I submit that there is probable cause to arrest John Daniel Macintyre (Y.O.B. 1989) for, on or about March 17, 2021 and dates prior thereto, a violation of 18 U.S.C. §§ 2252A(a)(5)(B), which prohibits a person from knowingly possessing or knowingly accessing with intent to view any material that contains any visual depiction involving the use of a minor engaging in sexually explicit conduct.

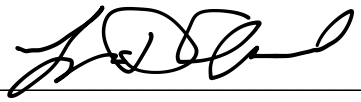
MICHAEL AGOSTINHO
Special Agent
Department of Homeland Security
Homeland Security Investigations

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by: Telephone.

(specify reliable electronic means)

March 17, 2021

Date



Judge's signature

Providence RI

City and State

Lincoln D Almond USMJ

Printed name and title